

WannaCry Made two Malaysian companies cried

Thursday, 18 May 2017 17:14

Two local companies have been hit by the infamous WannaCry ransomware, three days after the malicious software was released, infecting 200,000 computers in 150 countries so far.



According to IT security services company LGMS, the first case in Malaysia involved a director of one of its clients who came across the dreaded ransomware on his personal laptop on Saturday morning.

LGMS founder C.F. Fong said the data in the laptop had to be erased as the person did not intend to pay the US\$300 (RM1,300) ransom.

The same ransomware appeared in the machine of an automotive shop on Sunday morning.

“The company didn’t have any backup and might pay (the ransom),” said Fong.

Besides disconnecting computers from the network, there was not much else they could do, he noted.

As of 3pm yesterday, a website tracking incidences of WannaCry infections started showing blips in the Klang Valley area.

The website displays a blip whenever an infected computer pings its tracking servers, thus allowing it to map out a geographical distribution of the WannaCry infection.

Fong added that any machine infected by WannaCry should not be connected to a public or corporate network.

“Once you plug into any network, it will start spreading,” he pointed out.

Fong said none of LGMS’ clients, which include major banks in Malaysia, had reported any

problems so far, adding that he was quite confident that those who regularly updated their computers would not face any problems with WannaCry.

He said ransomware was not new but WannaCry had caused worldwide alarm because of how fast it was spreading.

“We have seen worse and devastating ransomware attacks before but WannaCry’s infection rate is one of the fastest ever as it exploits the vulnerability that exists in Windows,” Fong said.

Security companies all over the world are reporting an unprecedented wave of WannaCry ransomware infections since Friday when more than 150 countries were hit by it.

The ransomware encrypts the data on an infected computer, preventing users from accessing it.

According to a report in *The Guardian*, the ransomware uses a vulnerability first revealed as part of a leaked stash of NSA-related documents, which infects machines running Windows and encrypts their contents before demanding a ransom to decrypt these files.

The perpetrators promise to release the data once a ransom of US\$300 (RM1,300) is paid.

In just two days, computer networks of Britain’s National Health Service, Russia’s interior ministry and international shipper FedEx, among others, were affected.

The website tracking incidences of WannaCry infections was created by a 22-year-old British researcher known only as MalwareTech, who was credited with being an “accidental hero” after discovering a “kill switch” that halted WannaCry’s outbreak.

WannaCry Made two Malaysian companies cried

Thursday, 18 May 2017 17:14

Read more at

<http://www.thestar.com.my/news/nation/2017/05/16/wannacry-strikes-two-msian-companies-expert-first-organisation-infected-last-saturday/#V73CsGsG77fPAWyp.99>